We claim: 

CN 104/1036/2015.

1. An image forming apparatus, comprising:

a main body that includes a main controller capable of controlling operations of the image forming apparatus;

a consumable unit that is mounted on the main body; and

a Customer Replaceable Unit Monitoring, CRUM, chip that stores information regarding the consumable unit,

wherein the main controller transmits to the CRUM chip a first signal comprising first data and first integrity detection data regarding the first data for authentication with the CRUM chip,

wherein the CRUM chip tests integrity of the first signal using the first integrity detection data, in response to the first signal being received from the main controller, generates second integrity detection data using second data to be transmitted to the main controller and the first integrity detection data, in response to integrity of the first signal being verified, and transmits a second signal comprising the second data and the second integrity detection data to the main controller.

2. The image forming apparatus according to claim 1, wherein the main controller and the CRUM chip perform the authentication through a plurality of authentication processes,

wherein the main controller generates third integrity detection data using third data, the first integrity detection data, and the second integrity detection data in a final authentication process from among the plurality of authentication processes and transmits a third signal that includes the third data and the third integrity detection data to the CRUM chip,

wherein the CRUM chip finally tests the third signal using the third integrity detection data, in response to receiving the third signal, generates fourth integrity detection data using

fourth data and the first to third integrity detection data, in response to integrity of the third signal being verified, and transmits a fourth signal that includes the fourth data and the fourth integrity detection data to the main controller,

wherein the main controller finally tests the fourth signal using the fourth integrity detection data, in response to the fourth signal being received.

3. The image forming apparatus according to claim 2, wherein the plurality of authentication processes include a first authentication process in which the main controller and the CRUM chip transmit and receive the first signal and the second signal and generate a session key respectively, a second authentication process for synchronizing a first table stored in each of a main body of the image forming apparatus and the CRUM chip, a third authentication process for synchronizing a second table stored in each of the main body of the image forming apparatus and the CRUM chip, and a fourth authentication process in which the main controller and the CRUM chip transmit and receive the third signal and the fourth signal and determine compatibility between the image forming apparatus and the CRUM chip.

4. The image forming apparatus according to claim 2, wherein the main controller and the CRUM chip store integrity detection data used for the plurality of authentication processes respectively, and perform data communication, in response to the authentication being completed.

5. A CRUM chip communicable with an image forming apparatus, comprising:

an interface unit that receives a first signal including first data and first integrity detection data regarding the first data from a main body of the image forming apparatus;

a test unit that tests integrity of the signal using the first integrity detection data;

a generating unit that generates integrity detection data; and

a controller that controls operations of the test unit and the generating unit,

wherein the controller controls the generating unit to generate second integrity detection data using second data to be transmitted to a main body of the image forming apparatus and the first integrity detection data, in response to integrity of the first signal including the first integrity detection data being verified by the test unit, and transmits a second signal including the second data and the second integrity detection data to a main body of the image forming apparatus through the interface unit.

6. The CRUM chip according to claim 5, further comprising:

a storage for storing the first integrity detection data and the second integrity detection data.

7. The CRUM chip according to claim 6, wherein the controller controls the test unit to finally test third signal using the third integrity detection data, in response to receiving a third signal that includes third data and the third integrity detection data regarding the third data, controls the generating unit to generate fourth integrity detection data using fourth data to be transmitted to a main body of the image forming apparatus and the first to third integrity detection data, in response to integrity of the third signal being verified, and transmits a fourth signal that includes the fourth data and the fourth integrity detection data to a main body of the image forming apparatus through the interface unit.

8. The CRUM chip according to claim 6, wherein the controller generates a session key using the first data and the second data, and performs an authentication process for synchronizing a first table stored in each of a main body of the image forming apparatus and the CRUM chip, an authentication process for synchronizing a second table stored in

each of the main body of the image forming apparatus and the CRUM chip, and an authentication process for determining compatibility between the image forming apparatus and the CRUM chip based on at least one of the first table and the second table.

9. The CRUM chip according to claim 8, wherein the controller, in an authentication process for determining the compatibility, controls the test unit to perform a final test on all of the plurality of authentication process using the third integrity detection data, in response to a signal that includes third integrity detection data including both the first and second integrity detection data from the main body, and controls the generating unit to generate fourth integrity detection data which includes the first to third integrity detection data, in response to the final test result showing integrity, and transmits a signal including the fourth integrity detection data to the main body through the interface unit.

10. An authenticating method of an image forming apparatus, comprising:

generating first integrity detection data regarding first data by a main controller mounted on a main body of the image forming apparatus, for authentication with a CRUM chip;

transmitting by the main controller a first signal that includes the first data and the first integrity detection data to the CRUM chip;

testing integrity of the first signal by the CRUM chip using the first integrity detection data;

generating by the CRUM chip second integrity detection data using second data to be transmitted to the main controller and the first integrity detection data, in response to integrity of the first signal being verified; and

transmitting by the CRUM chip a second signal that includes the second data and the second integrity detection data to the main controller.

11. The method according to claim 10, further comprising:

generating by the main controller third integrity detection data using third data, the first integrity detection data and the second integrity detection data and transmitting a third signal that includes the third data and the third integrity detection data to the CRUM chip;

finally testing the third signal by the CRUM chip using the third integrity detection data, generating fourth integrity detection data using fourth data and the first to third integrity detection data in response to integrity of the third signal being verified, and transmitting fourth signal that includes the fourth data and the fourth integrity detection data to the main controller; and

finally testing by the main controller the fourth signal using the fourth integrity detection data, in response to the fourth signal being received.

12. The method according to claim 11, further comprising:

performing by the main controller an authentication process for synchronizing a first table stored in each of a main body of the image forming apparatus and the CRUM chip and an authentication process for synchronizing a second table stored in each of a main body of the image forming apparatus and the CRUM chip, after receiving the second signal and before transmitting the third signal,

wherein the first and second data are data for generating a session key, and the third and fourth data are data for determining compatibility between a main body of the image forming apparatus and the CRUM chip.

13. An authenticating method of a CRUM chip communicable with an image forming apparatus, comprising:

receiving from a main body of the image forming apparatus a first signal that includes

first data and first integrity detection data regarding the first data;

testing integrity of the first signal using the first integrity detection data;

generating second integrity detection data using second data to be transmitted to a main body of the image forming apparatus and the first integrity detection data; and

transmitting a second signal that includes the second data and the second integrity detection data to a main body of the image forming apparatus.

14. The method according to claim 13, further comprising:

storing the first and second integrity detection data.

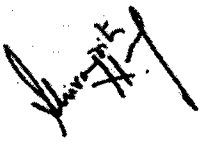
15. The method of claim 14, further comprising:

finally testing the third signal using the third integrity detection data in response to third signal that includes third data and third integrity detection data regarding the third data being received from a main body of the image forming apparatus;

generating fourth integrity detection data using fourth data to be transmitted to a main body of the image forming apparatus and the first to third integrity detection data, in response to integrity of the third signal being verified; and

transmitting fourth signal that includes the fourth data and the fourth integrity detection data to a main body of the image forming apparatus.

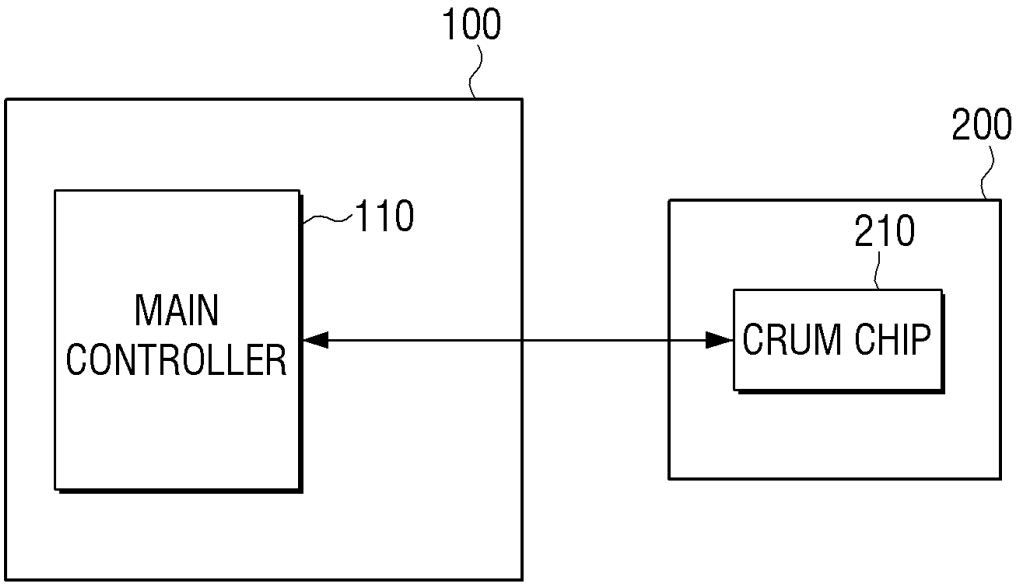
Dated this 24th day of July, 2013.



(SHIVARPITA NAILWAL)

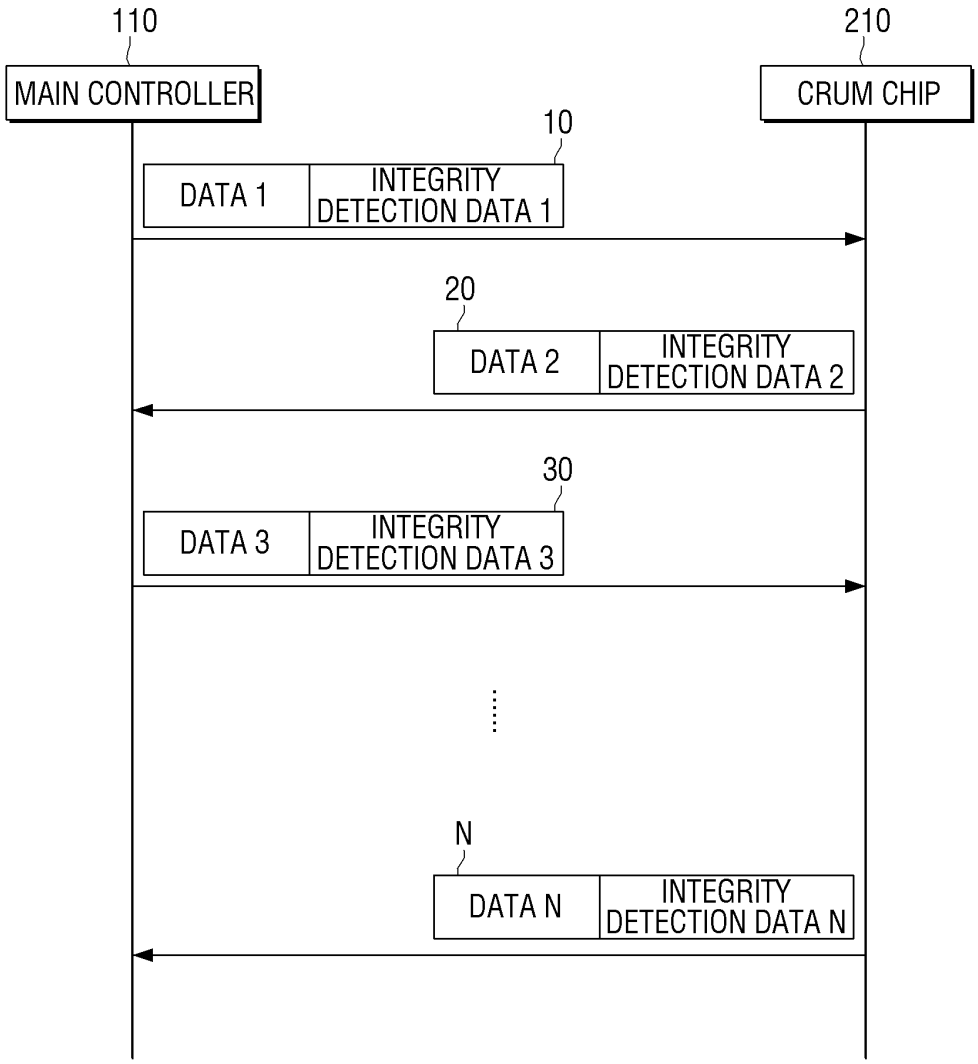
PATENT AGENT

FIG. 1



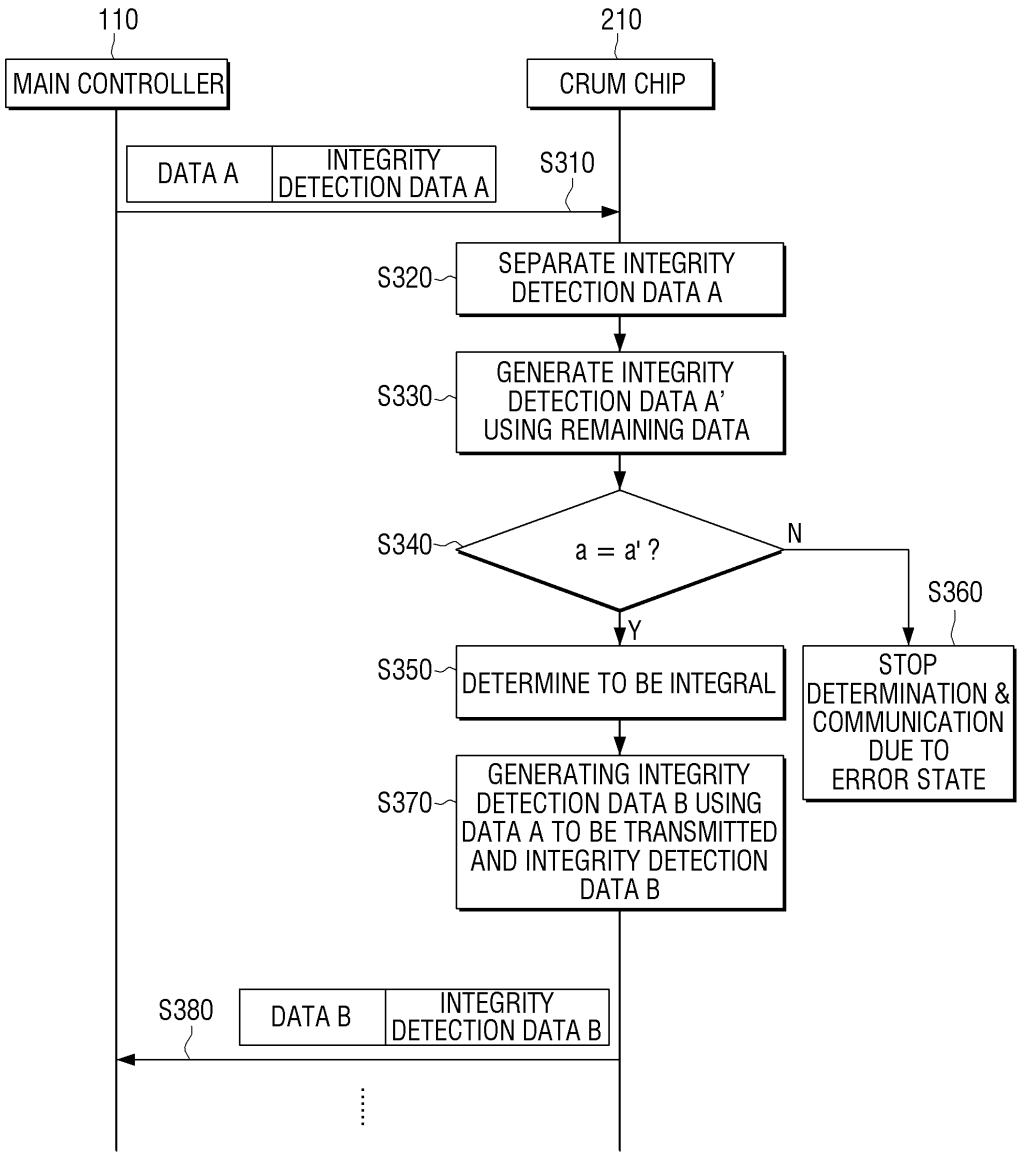
(Chetan Chadha)
Patent Agent for the Applicant

FIG. 2



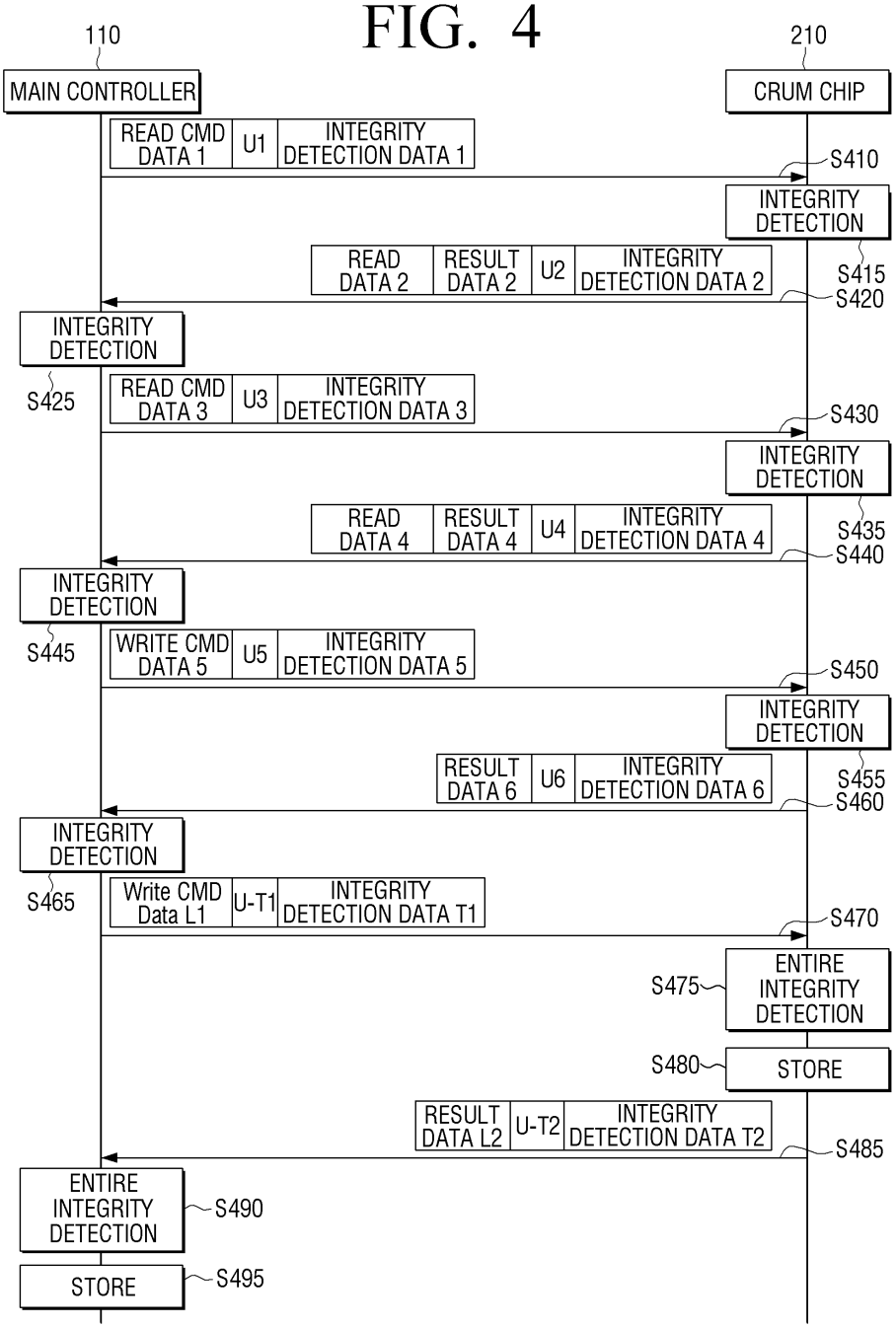
(Chetan Chadha)
Patent Agent for the Applicant

FIG. 3



(Chetan Chadha)
Patent Agent for the Applicant

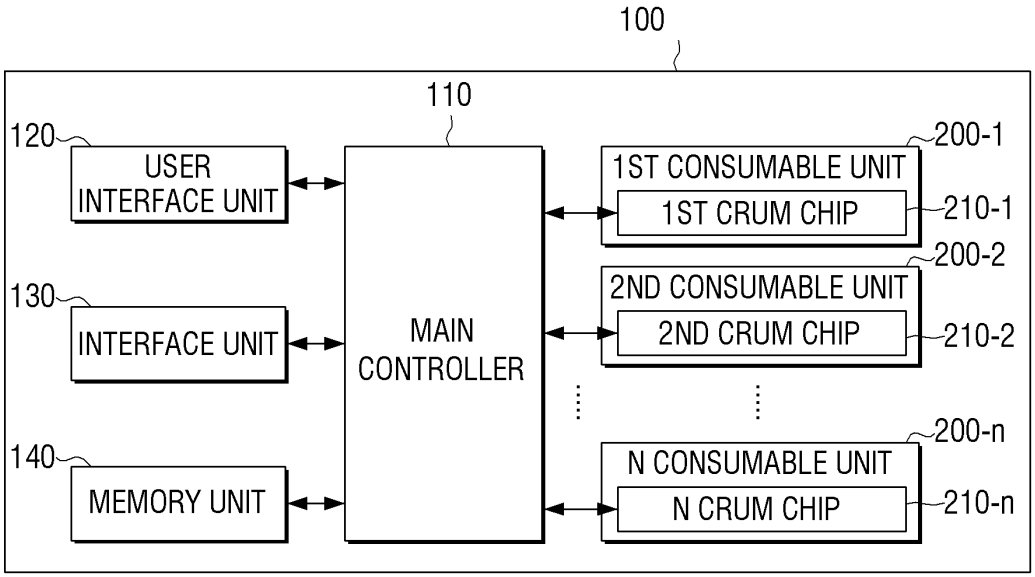
FIG. 4



(Chetan Chadha)

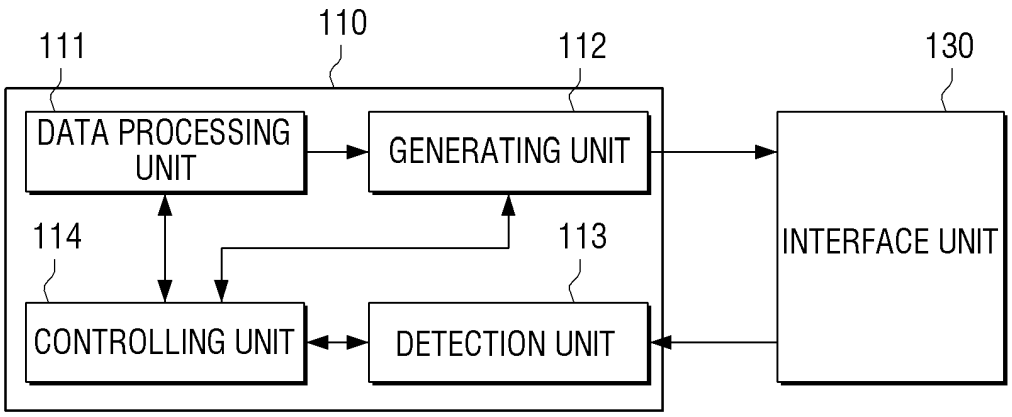
Patent Agent for the Applicant

FIG. 5



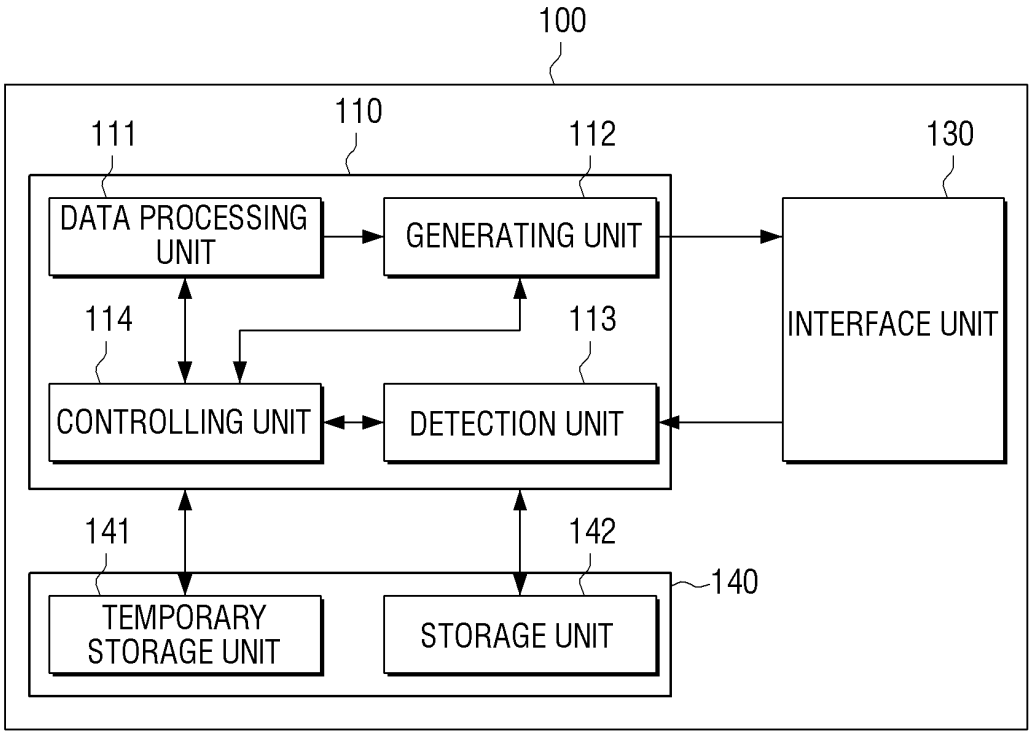
(Chetan Chadha)
Patent Agent for the Applicant

FIG. 6



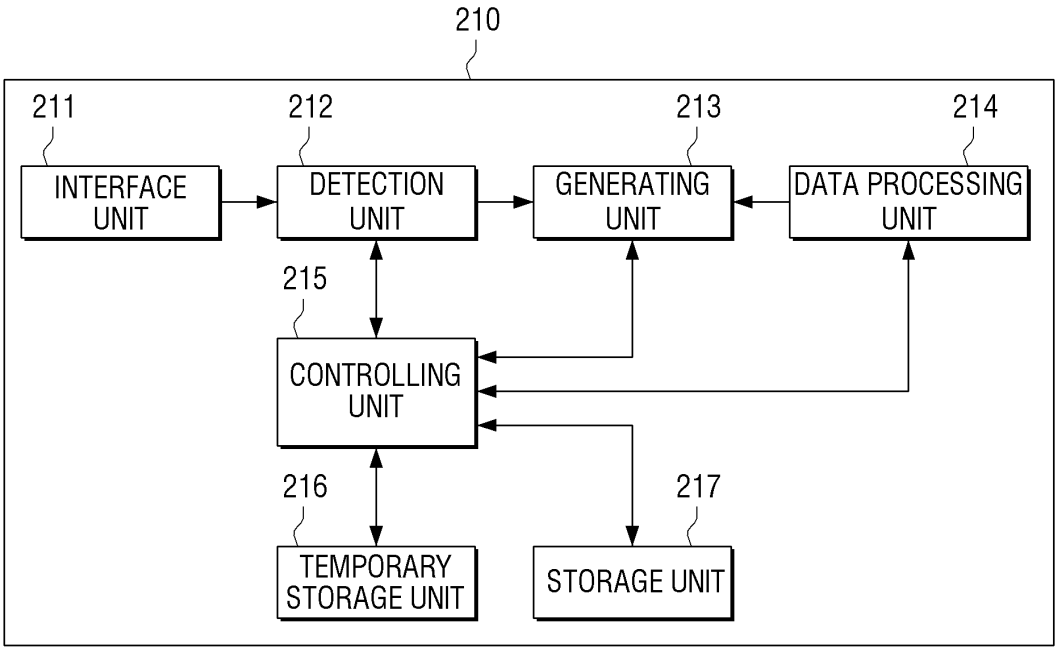
(Chetan Chadha)
Patent Agent for the Applicant

FIG. 7



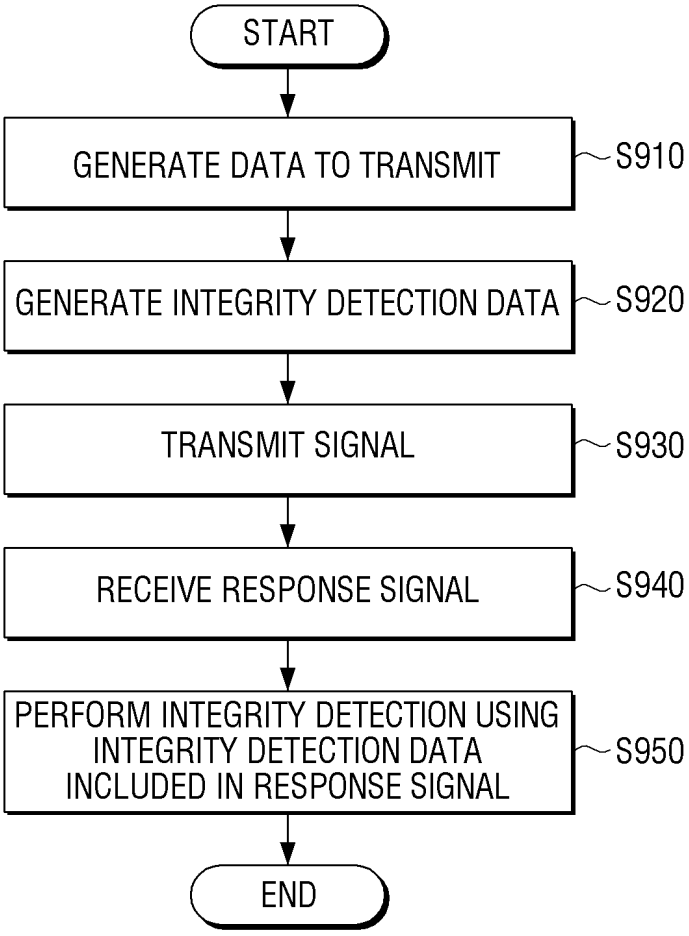
(Chetan Chadha)
Patent Agent for the Applicant

FIG. 8



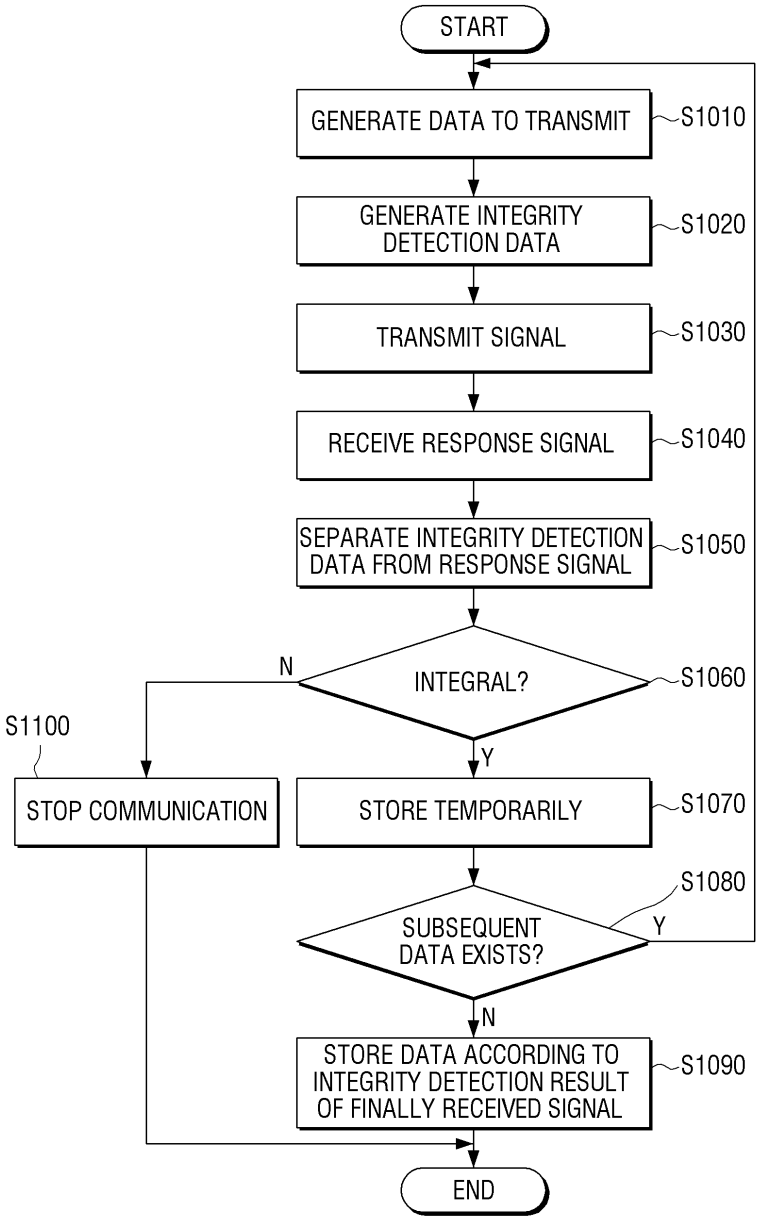
(Chetan Chadha)
Patent Agent for the Applicant

FIG. 9



(Chetan Chadha)
Patent Agent for the Applicant

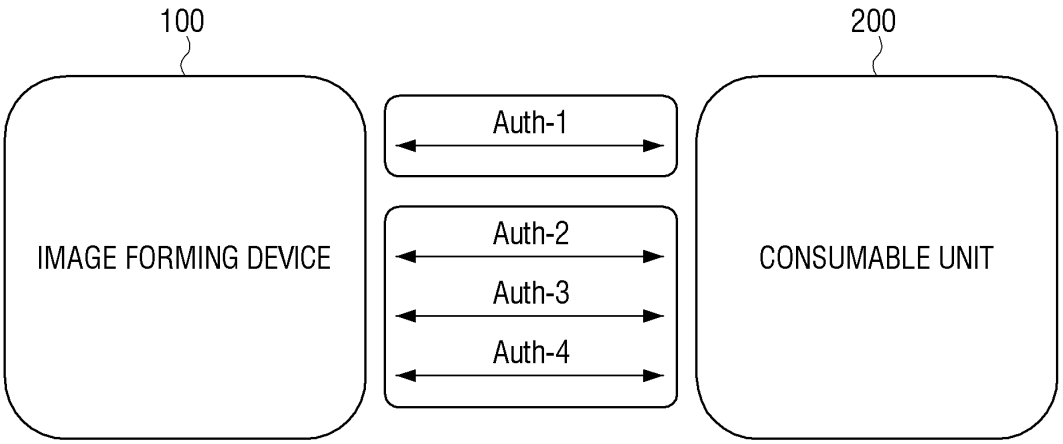
FIG. 10



(Chetan Chadha)

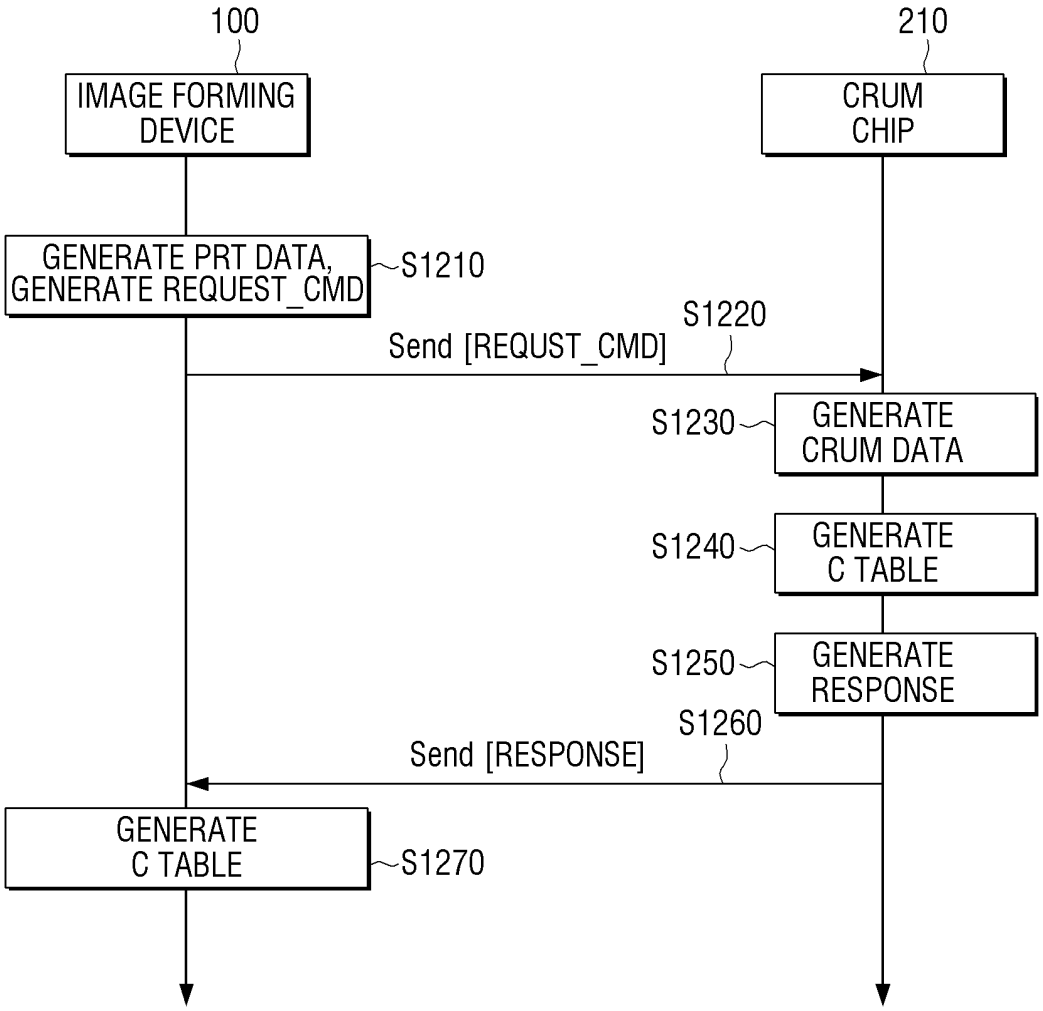
Patent Agent for the Applicant

FIG. 11



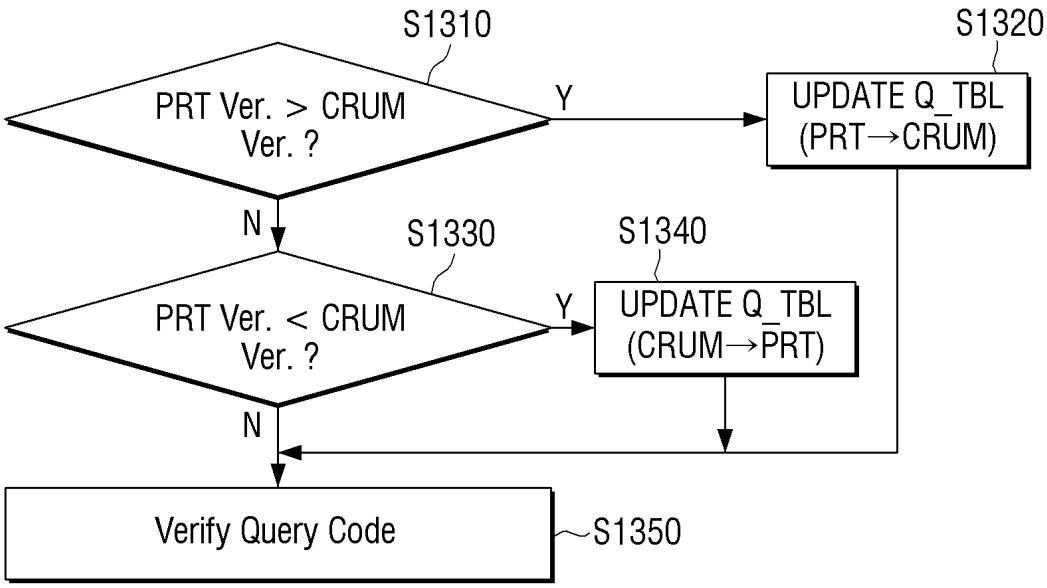
(Chetan Chadha)
Patent Agent for the Applicant

FIG. 12



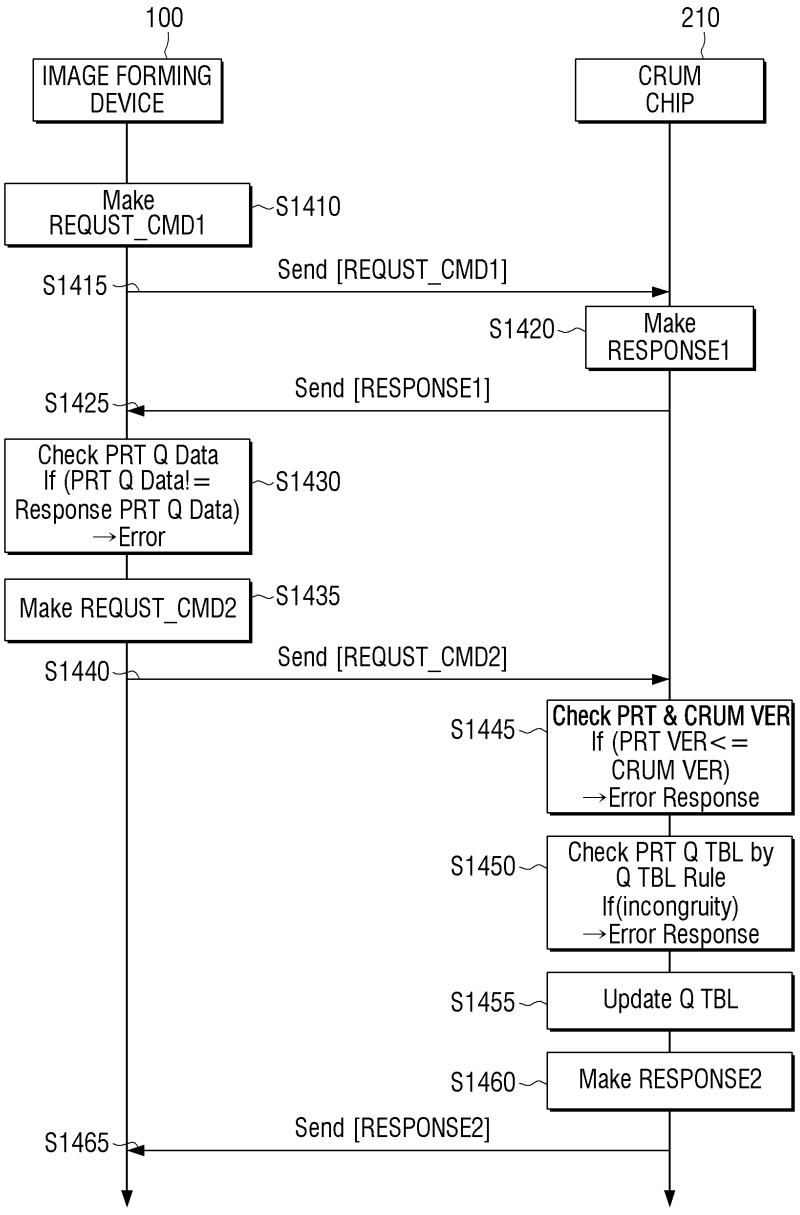
(Chetan Chadha)
Patent Agent for the Applicant

FIG. 13



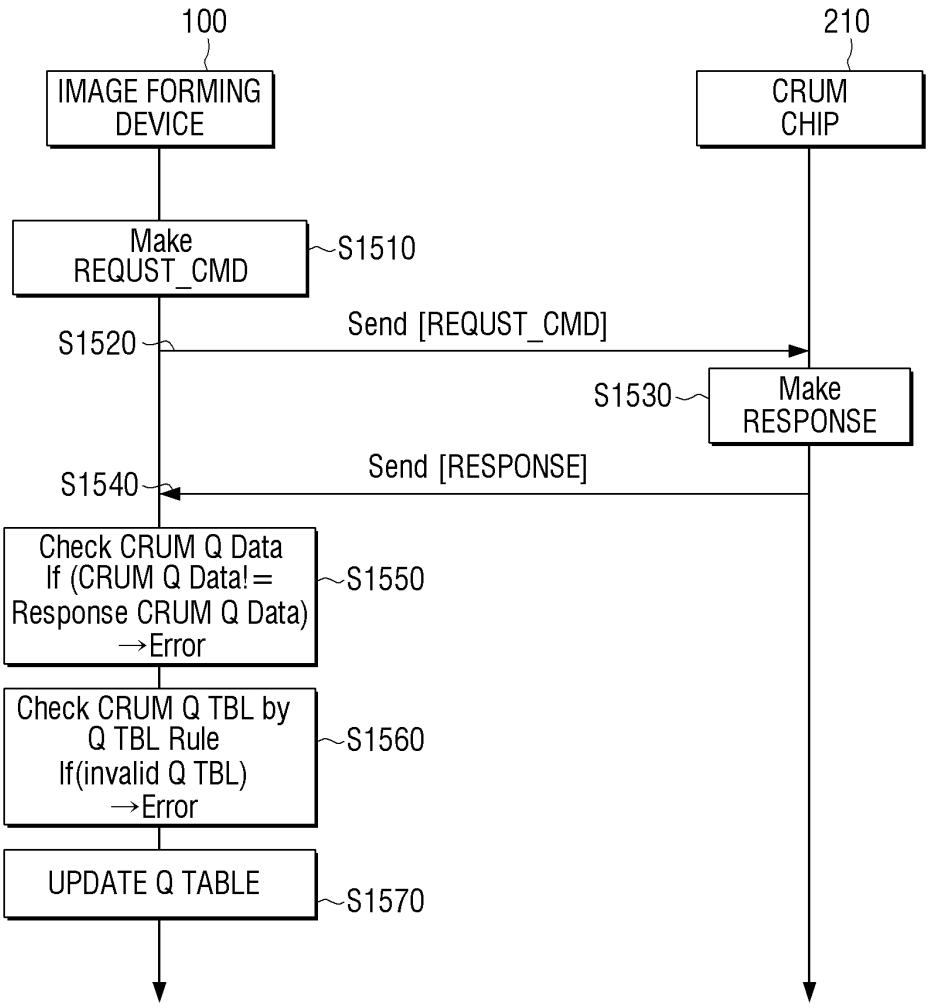
(Chetan Chadha)
Patent Agent for the Applicant

FIG. 14



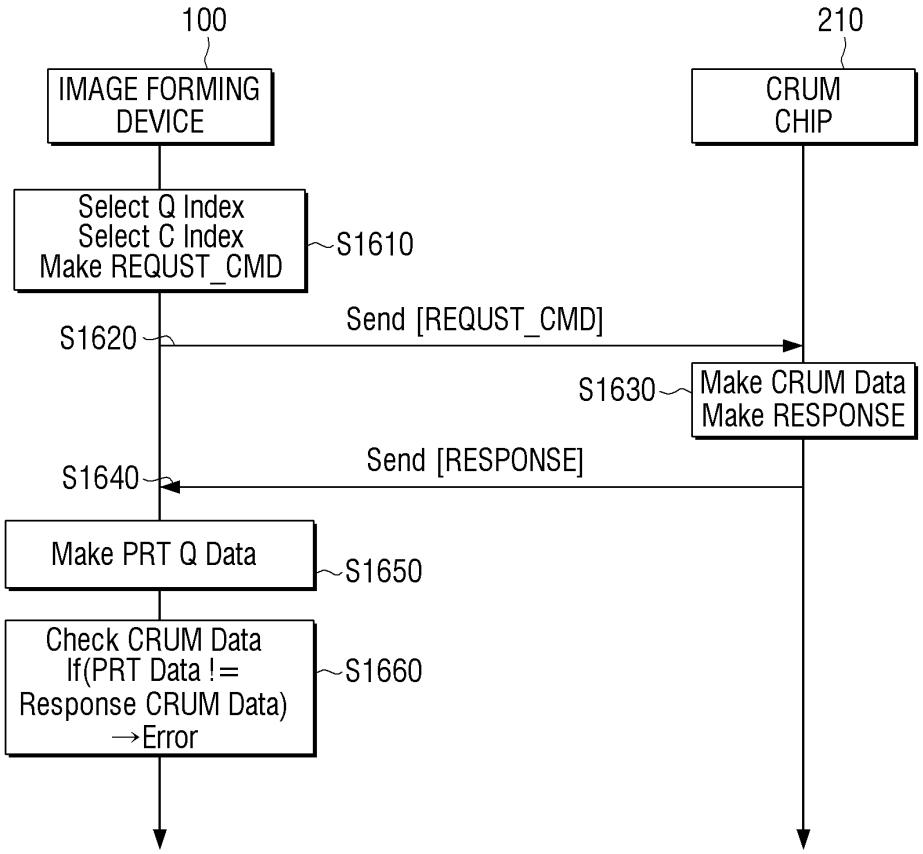
(Chetan Chadha)
Patent Agent for the Applicant

FIG. 15



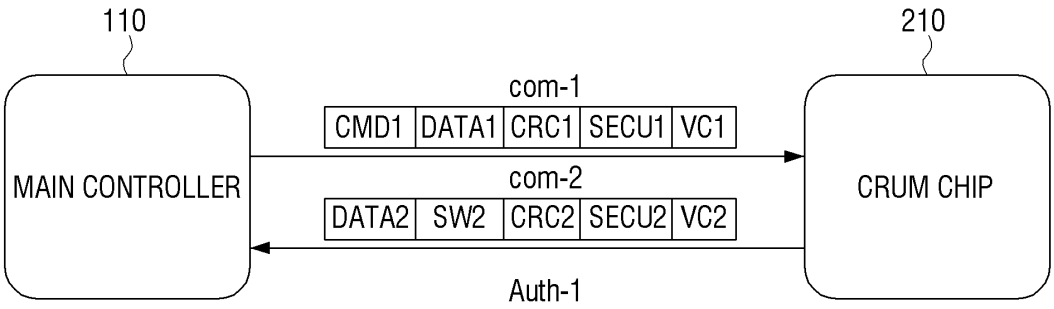
(Chetan Chadha)
Patent Agent for the Applicant

FIG. 16



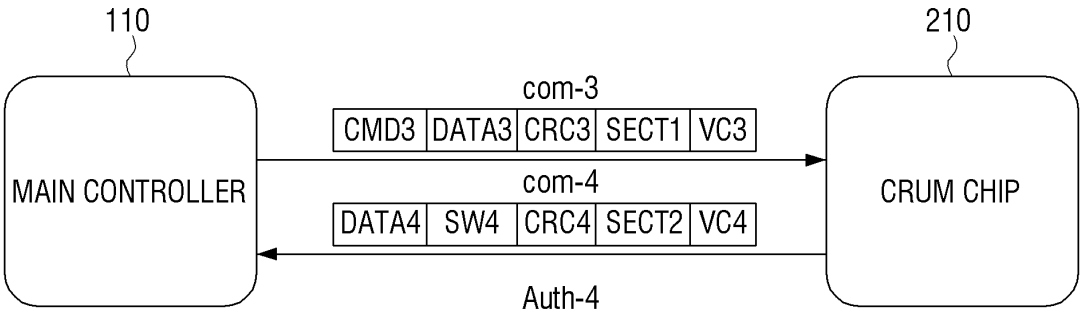
(Chetan Chadha)
Patent Agent for the Applicant

FIG. 17



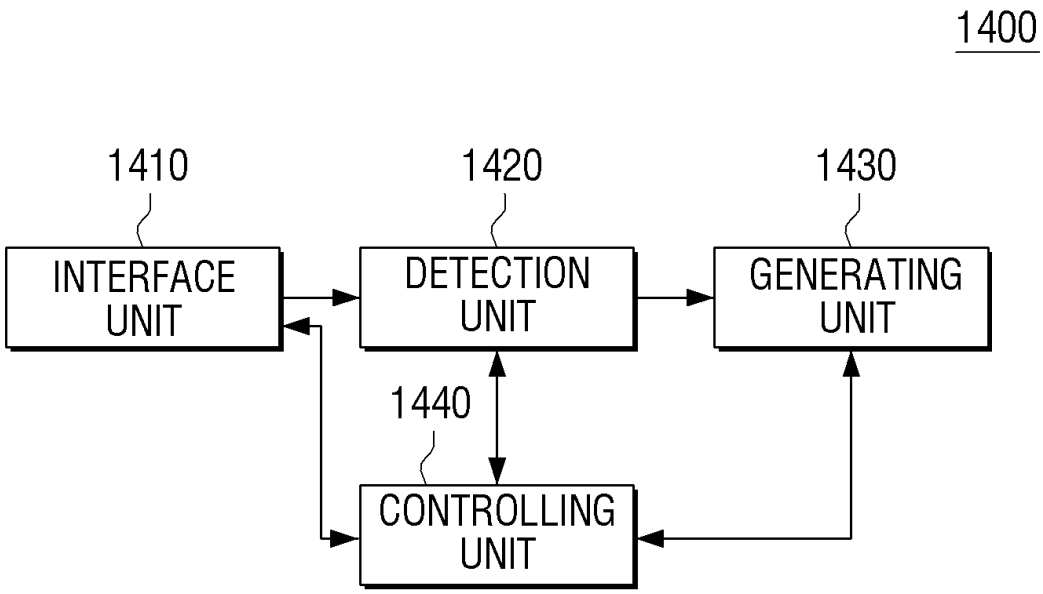
(Chetan Chadha)
Patent Agent for the Applicant

FIG. 18



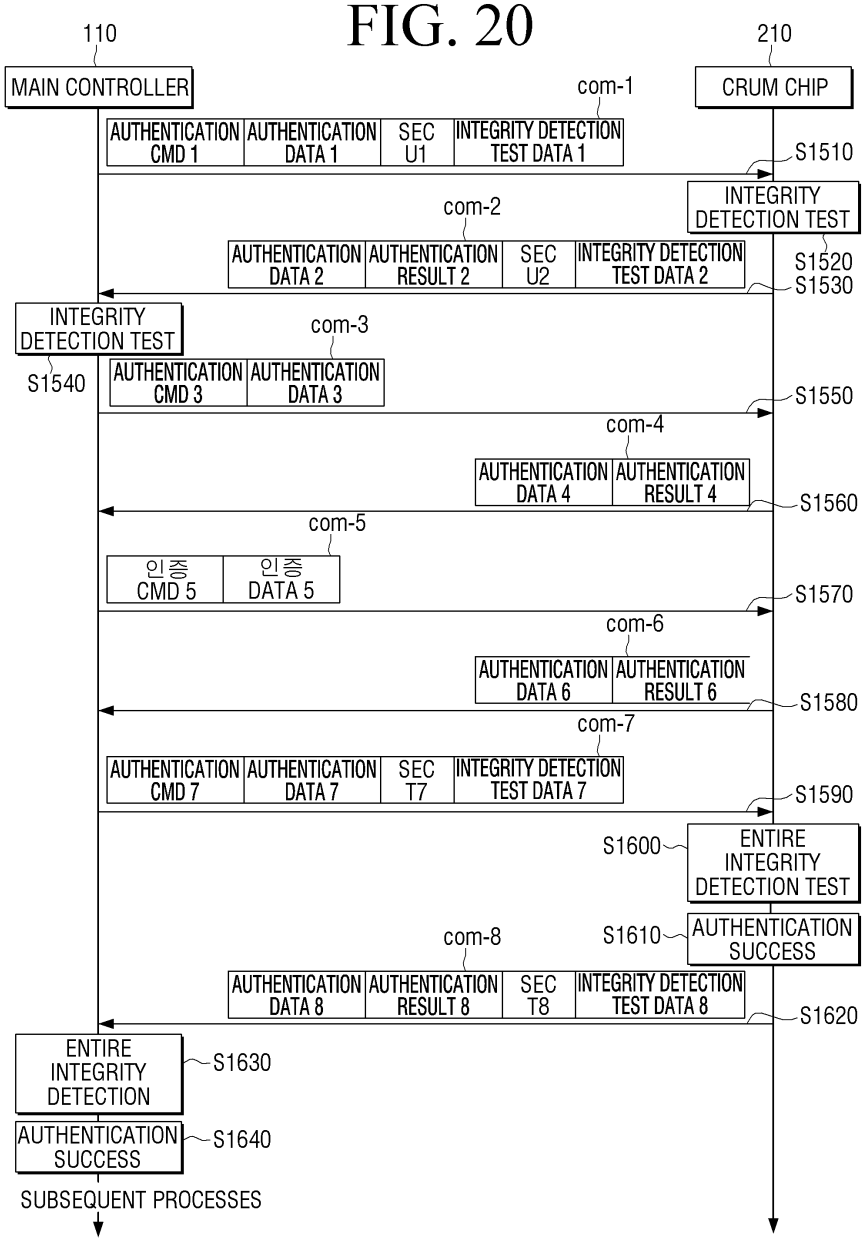
(Chetan Chadha)
Patent Agent for the Applicant

FIG. 19



(Chetan Chadha)
Patent Agent for the Applicant

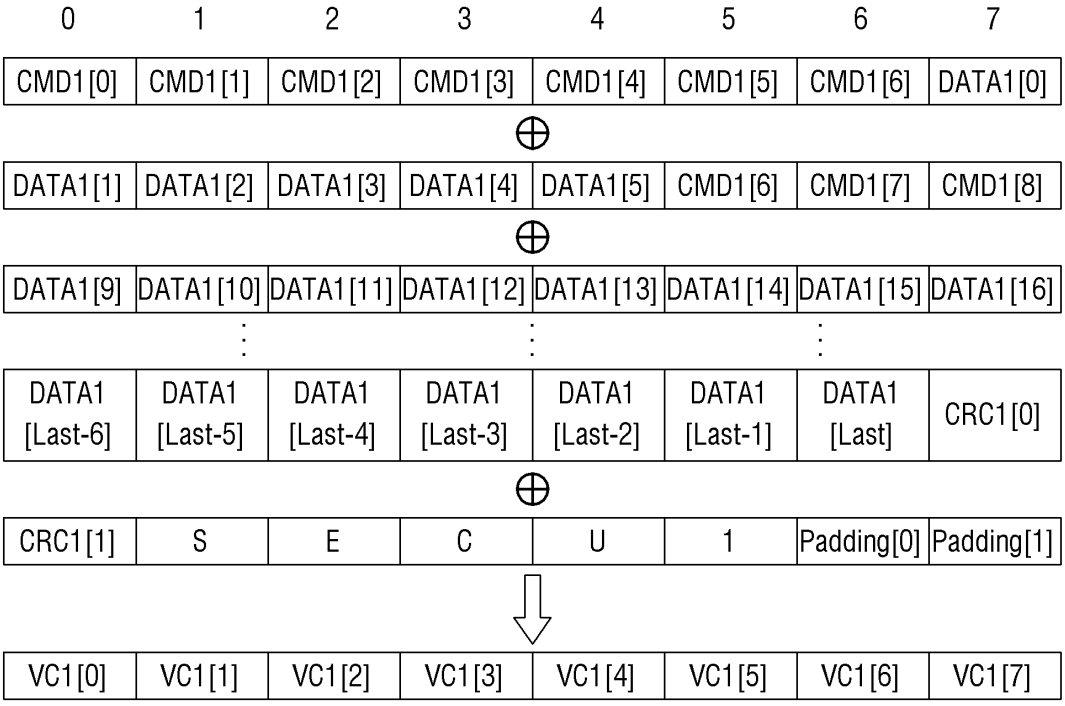
FIG. 20



(Chetan Chadha)

Patent Agent for the Applicant

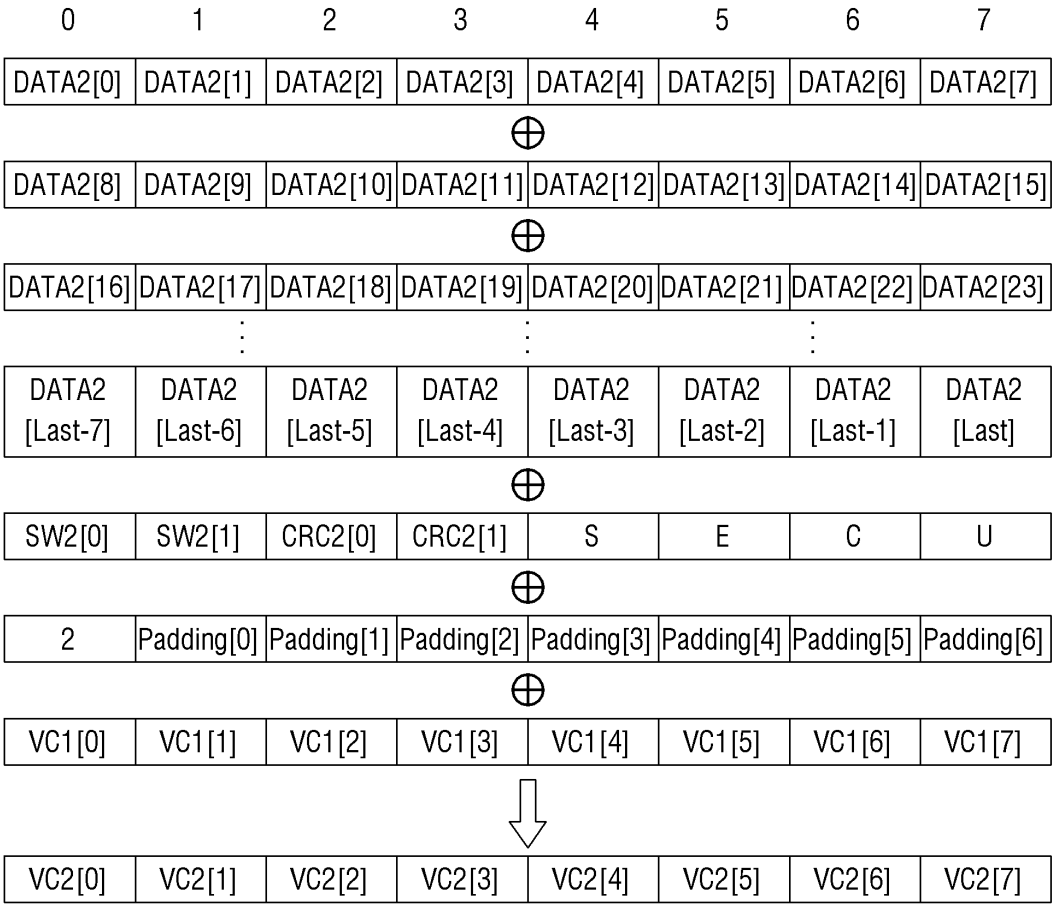
FIG. 21



(Chetan Chadha)

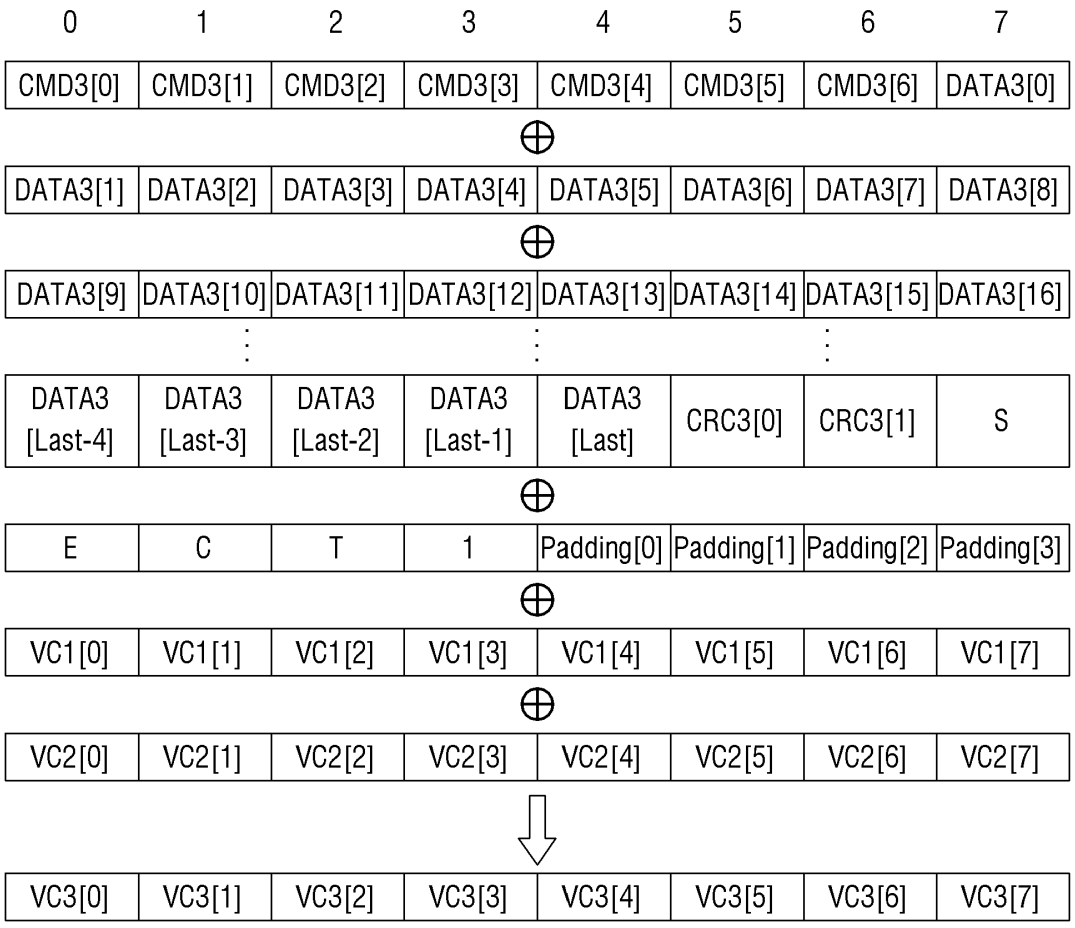
Patent Agent for the Applicant

FIG. 22



(Chetan Chadha)
Patent Agent for the Applicant

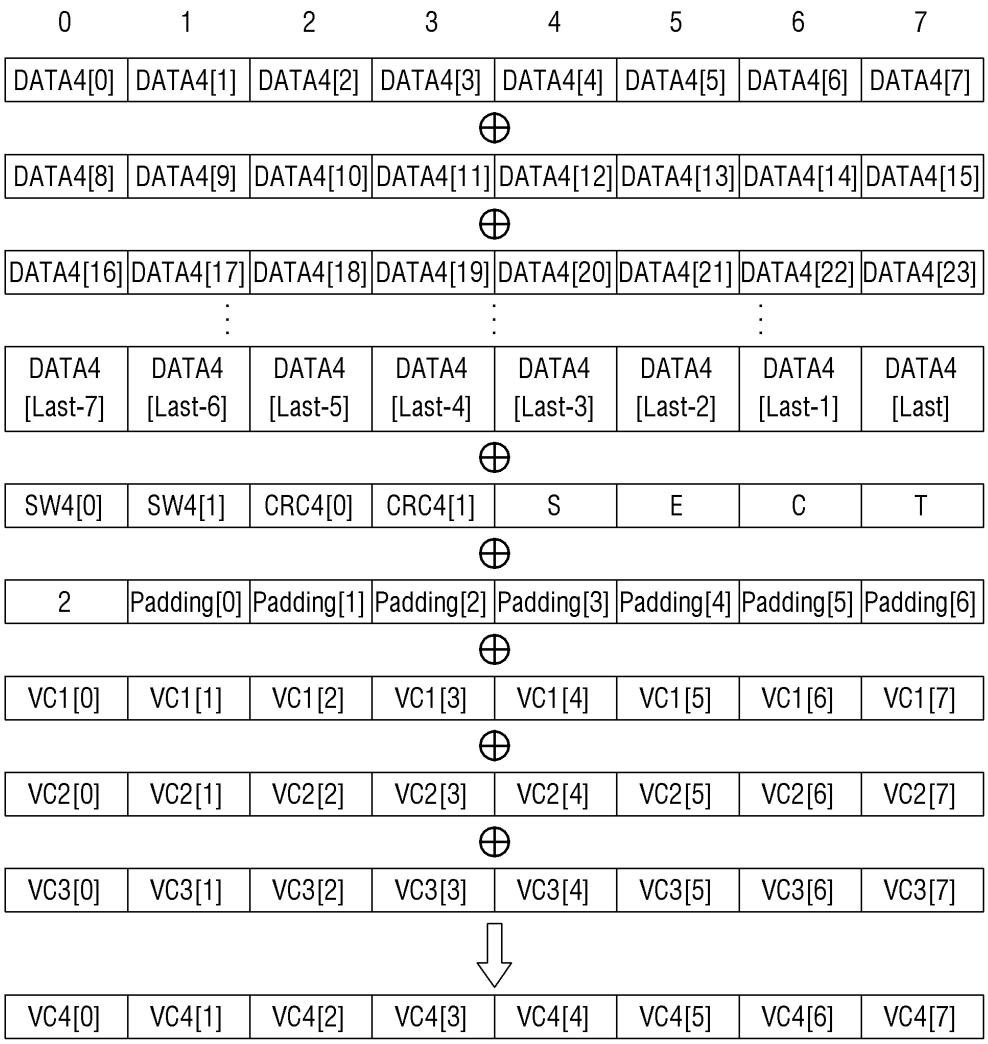
FIG. 23



(Chetan Chadha)

Patent Agent for the Applicant

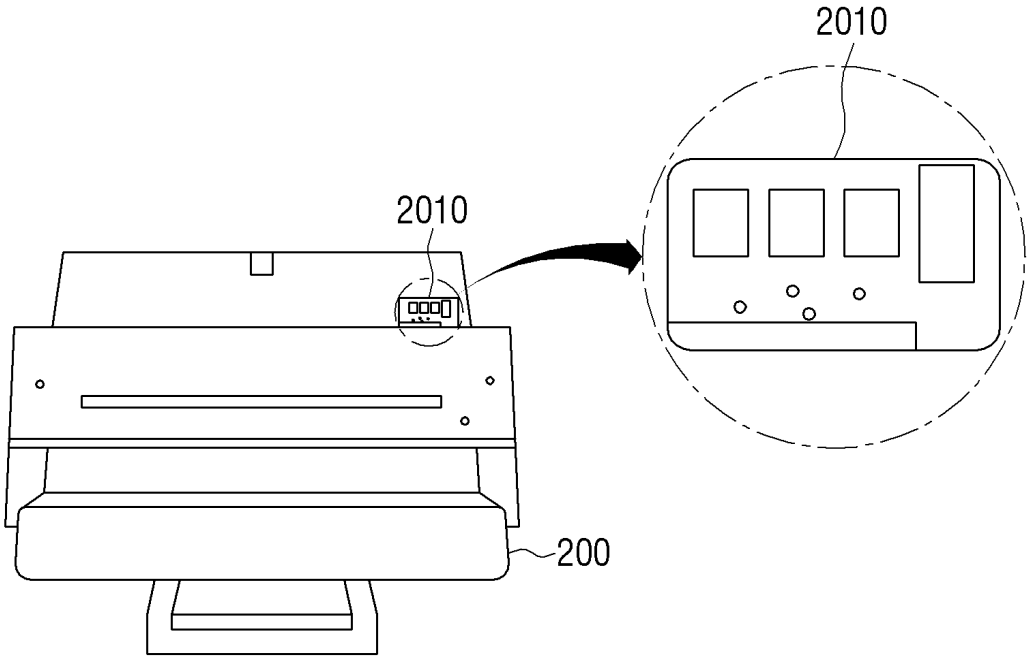
FIG. 24



(Chetan Chadha)

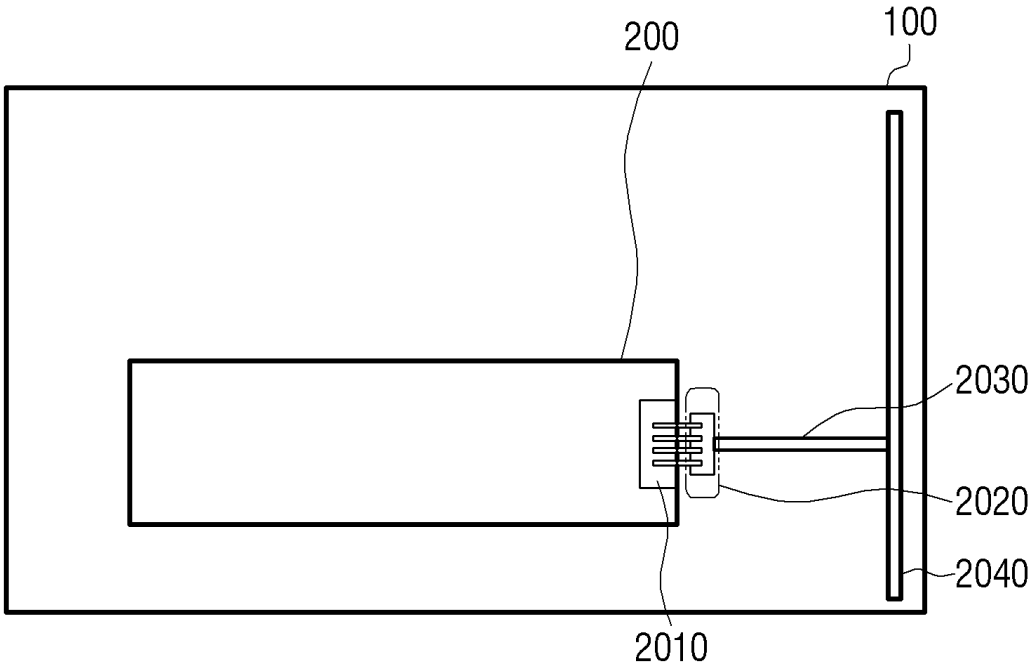
Patent Agent for the Applicant

FIG. 25



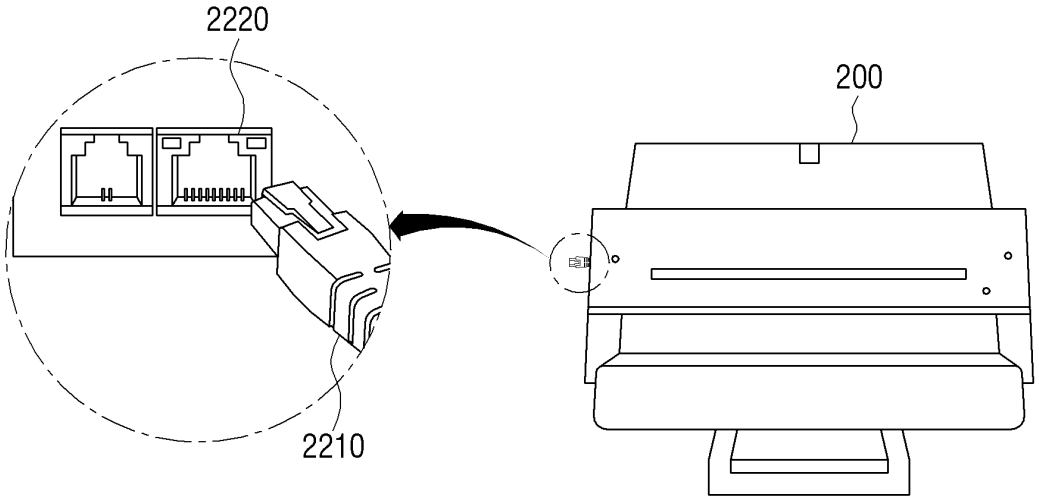
(Chetan Chadha)
Patent Agent for the Applicant

FIG. 26



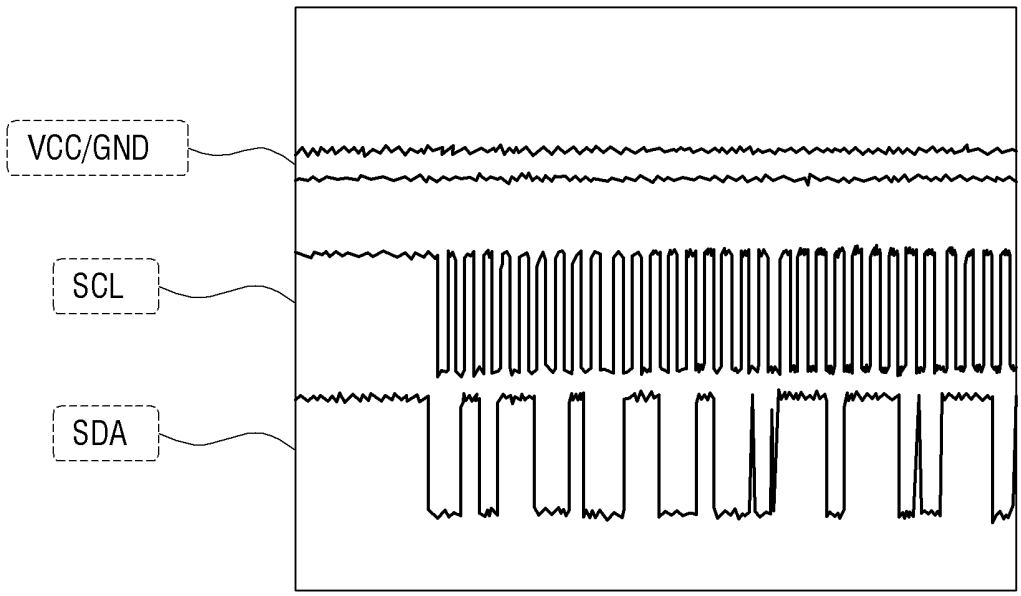
(Chetan Chadha)
Patent Agent for the Applicant

FIG. 27



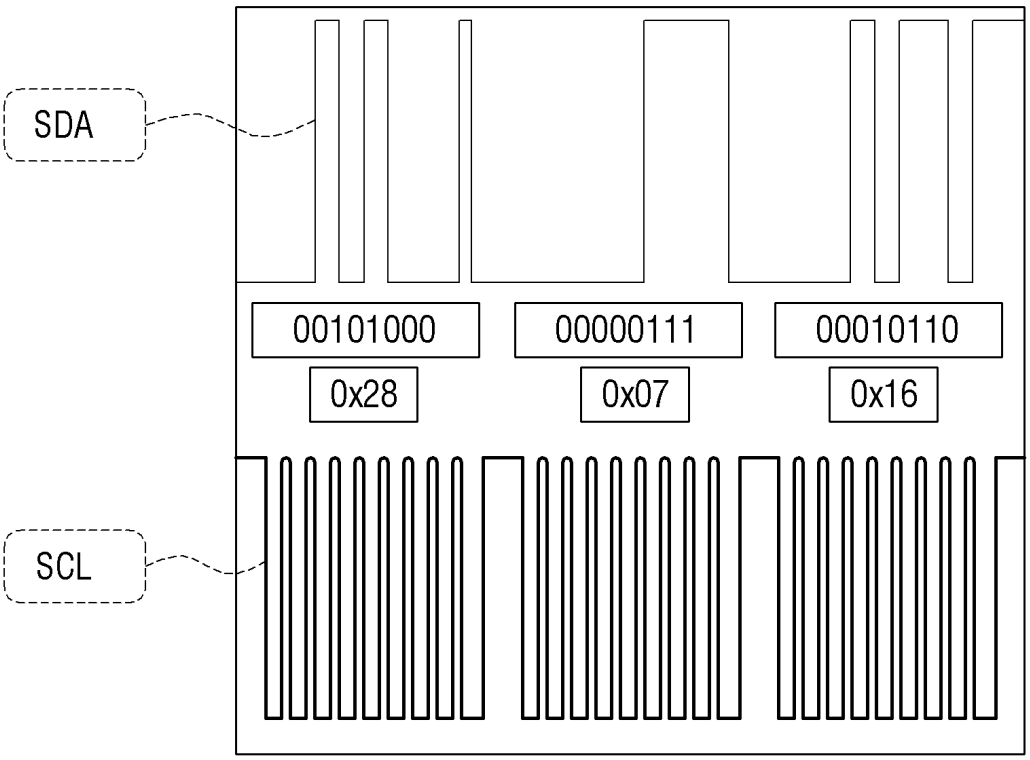
(Chetan Chadha)
Patent Agent for the Applicant

FIG. 28



(Chetan Chadha)
Patent Agent for the Applicant

FIG. 29



(Chetan Chadha)
Patent Agent for the Applicant